FIPS 140-3 and beyond

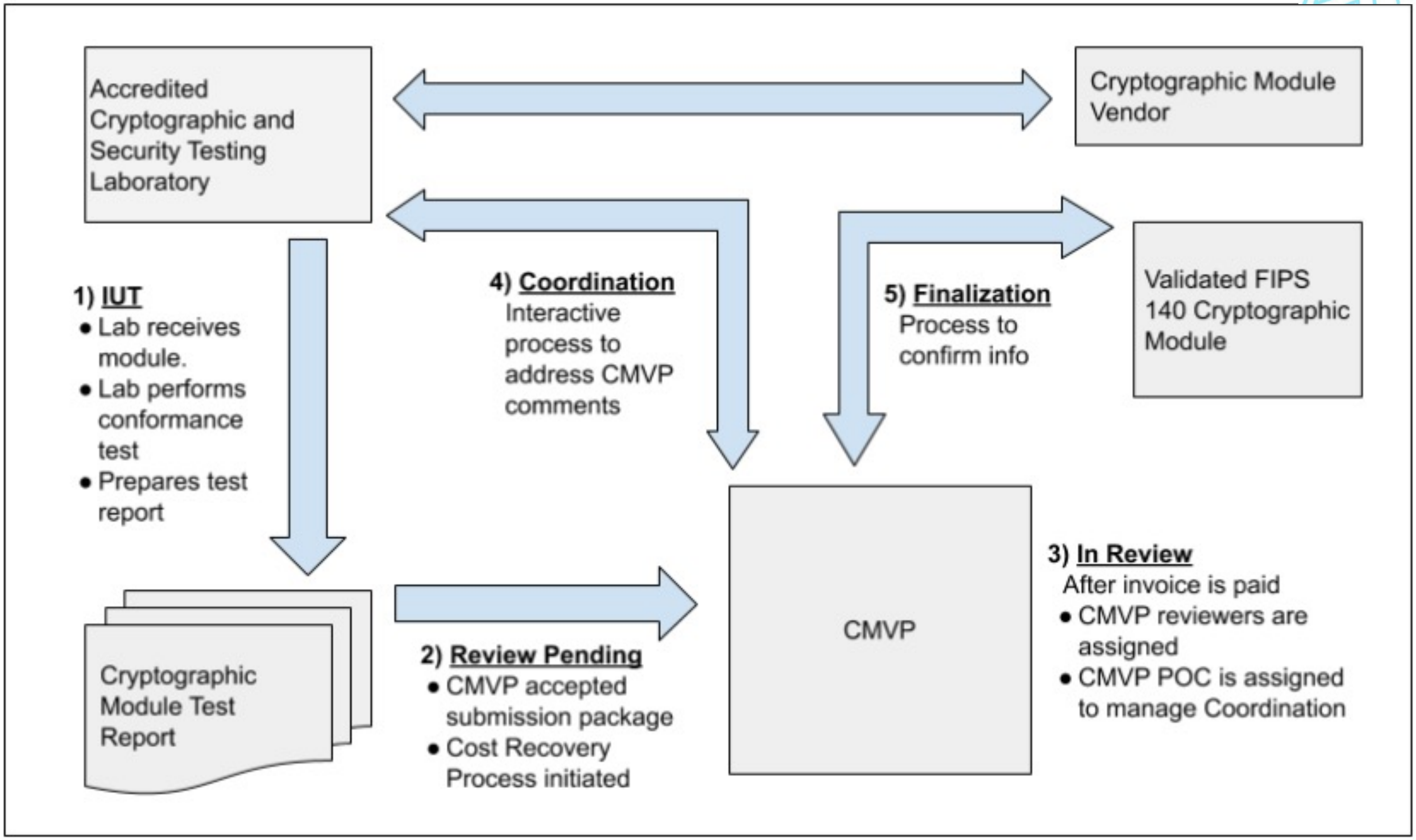
Swapneela Unkule, CST Lab Manager
atsec information security corp.
Email: swapneela@atsec.com

atsec bootcamp 2024, February 2027

Topics Covered

- ❖ FIPS 140-3 validation process
- ❖ FIPS 140-3 status
- ❖ Steps taken for process Improvement
- ❖ CMVP automation

FIPS 140-3 validation process



Accredited Cryptographic and Security Testing Laboratory

Cryptographic Module Vendor

1) **IUT**
- Lab receives module.
- Lab performs conformance test
- Prepares test report

4) **Coordination**
Interactive process to address CMVP comments

5) **Finalization**
Process to confirm info

Validated FIPS 140 Cryptographic Module

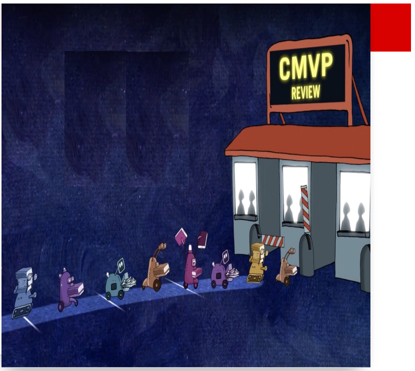
Cryptographic Module Test Report

2) **Review Pending**
- CMVP accepted submission package
- Cost Recovery Process initiated

CMVP

3) **In Review**
After invoice is paid
- CMVP reviewers are assigned
- CMVP POC is assigned to manage Coordination

FIPS 140-3 status



- 140-3 validation began on 22nd September **2020**

- In the last three years, only **14** modules have been certified.

- Currently there are **281** modules in the Modules in Process List (MIP).

- **130** submissions are in Review Pending i.e., waiting to be reviewed.

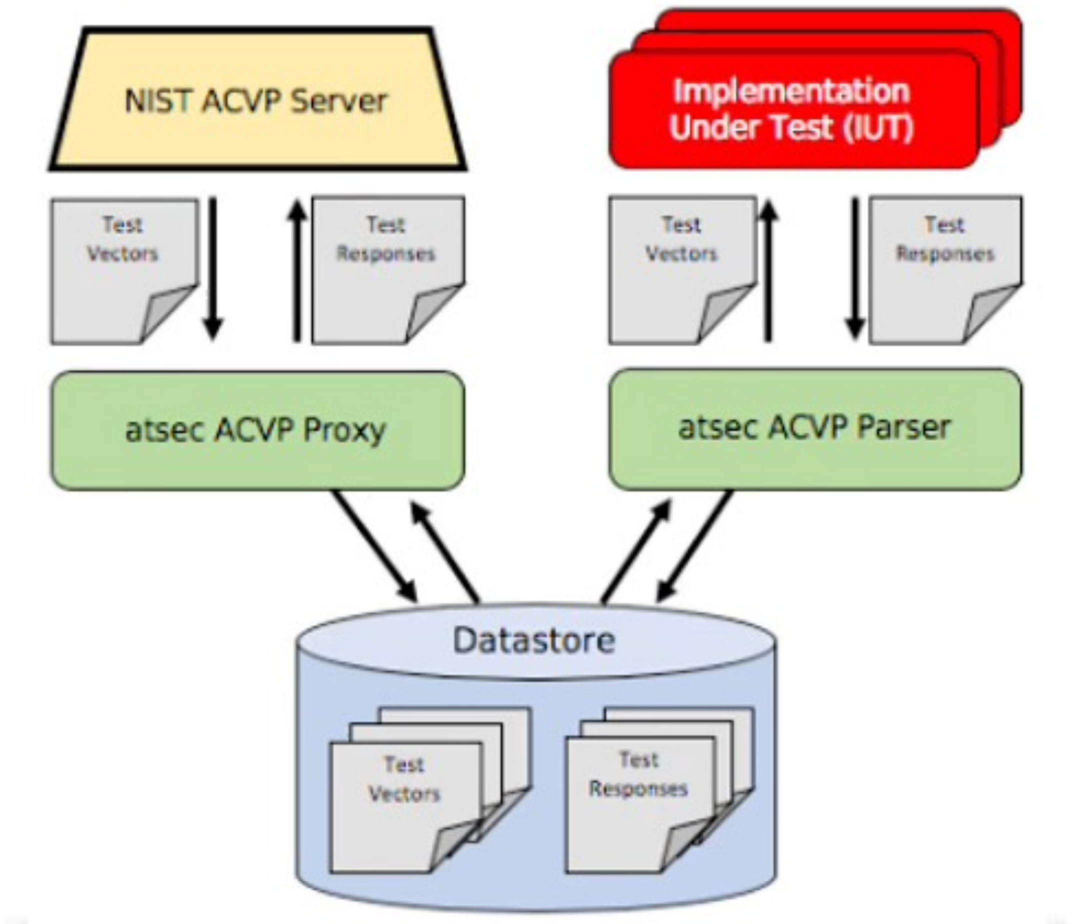
- All FIPS 140-2 modules will be on historical list in September 2026.

Steps taken for process Improvement

CMVP is continuously working on new programs for improving the validation process. Some of these include:

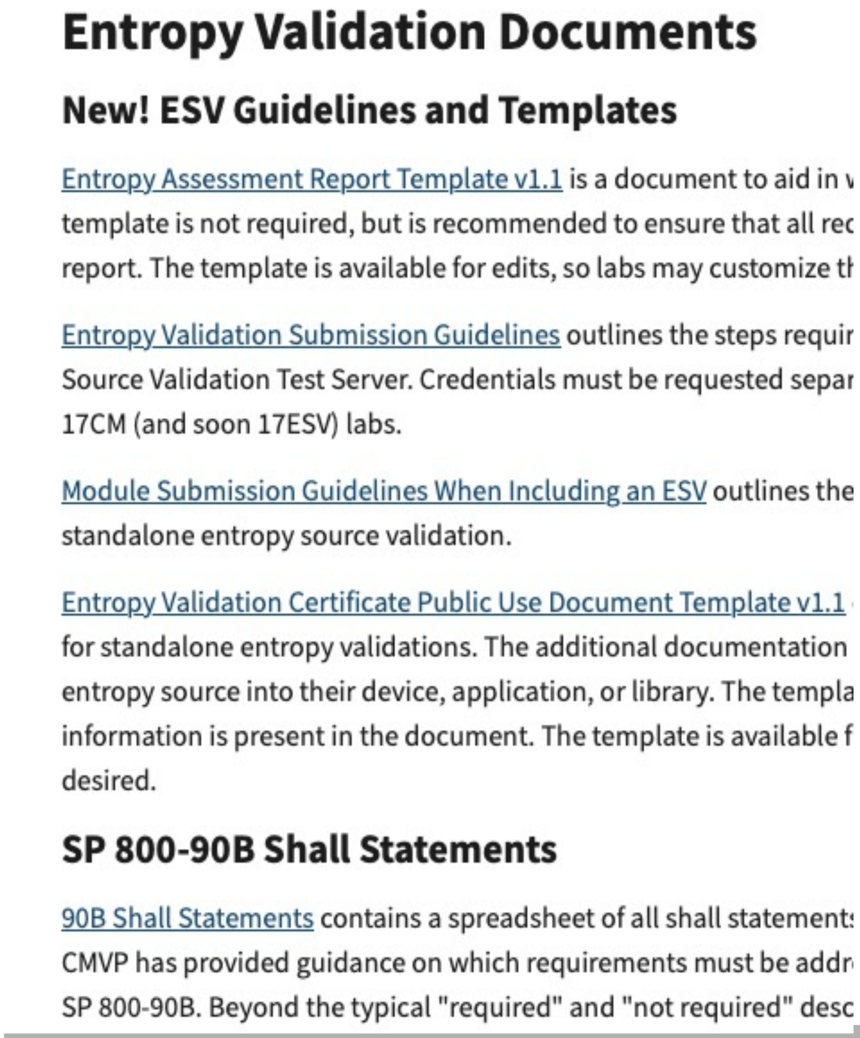
- Automated Cryptographic Validation Test System (ACVTS)
- Entropy Source Validation Program (ESV)
- Web Cryptik launched for report writing and submission
- SP 800-140Brev1 published recently with module verification tool.

Automated Cryptographic Validation Test System (ACVTS)



- Program launched in 2019.
- 4000+ validations so far.
- Demo and Production server available for testing.
- Certification within less than a week after submission.

Entropy Source Validation Program (ESV)



Entropy Validation Documents

New! ESV Guidelines and Templates

Entropy Assessment Report Template v1.1 is a document to aid in v template is not required, but is recommended to ensure that all rec report. The template is available for edits, so labs may customize th

Entropy Validation Submission Guidelines outlines the steps requir Source Validation Test Server. Credentials must be requested separ 17CM (and soon 17ESV) labs.

Module Submission Guidelines When Including an ESV outlines the standalone entropy source validation.

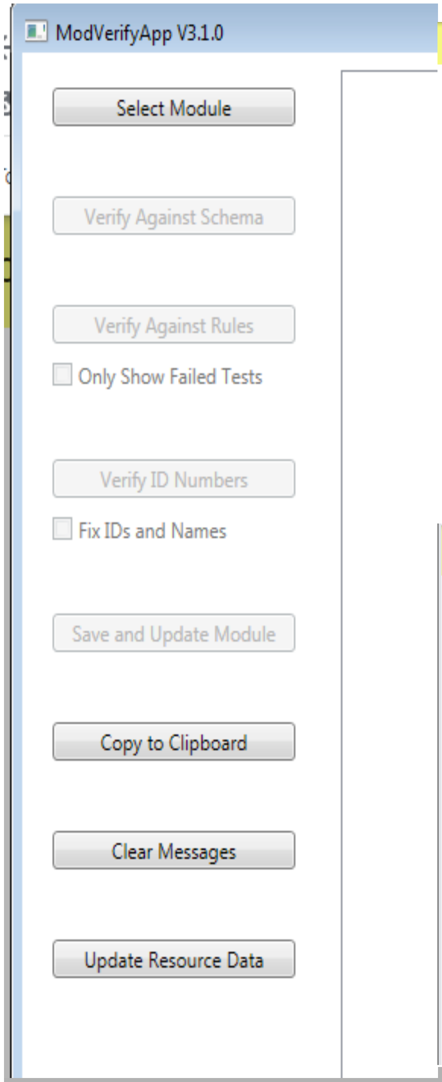
Entropy Validation Certificate Public Use Document Template v1.1 for standalone entropy validations. The additional documentation entropy source into their device, application, or library. The templa information is present in the document. The template is available f desired.

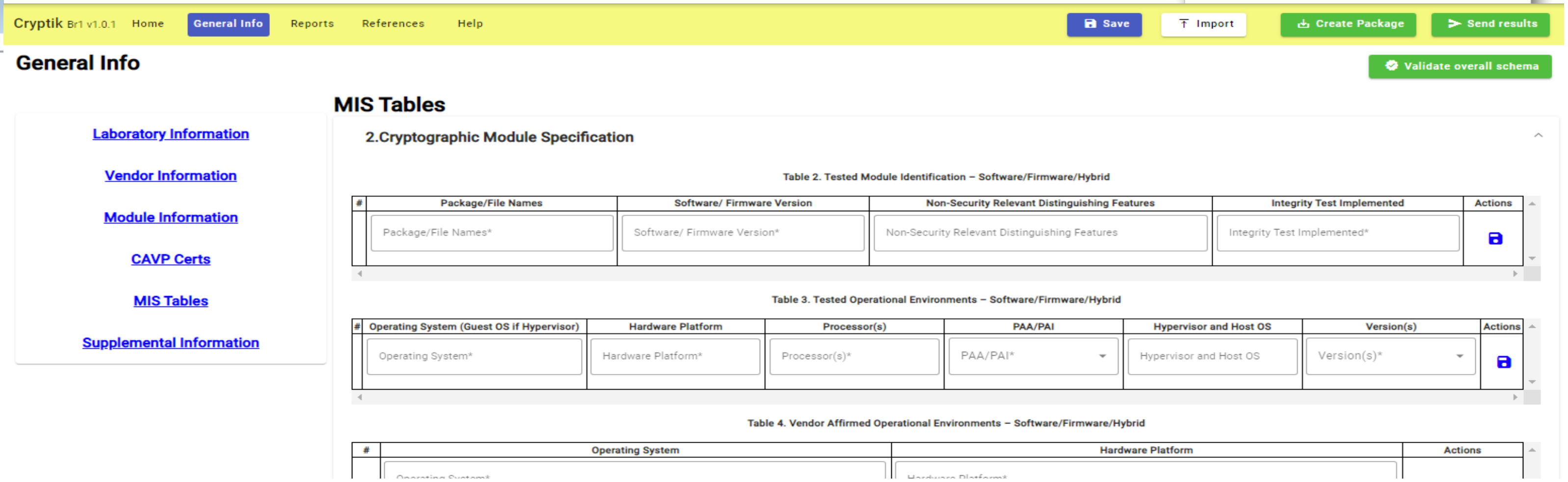
SP 800-90B Shall Statements

90B Shall Statements contains a spreadsheet of all shall statement CMVP has provided guidance on which requirements must be addr SP 800-90B. Beyond the typical "required" and "not required" desc

- ESV became mandatory in January **2022.**
- **121** entropy source validations so far.
- Statistical testing via NIST ESV server.
- 1–2-months certification time after submission.

Web Cryptik and Verification tool





General Info

MIS Tables

- Laboratory Information
- Vendor Information
- Module Information
- CAVP Certs
- MIS Tables
- Supplemental Information

2.Cryptographic Module Specification

Table 2. Tested Module Identification – Software/Firmware/Hybrid

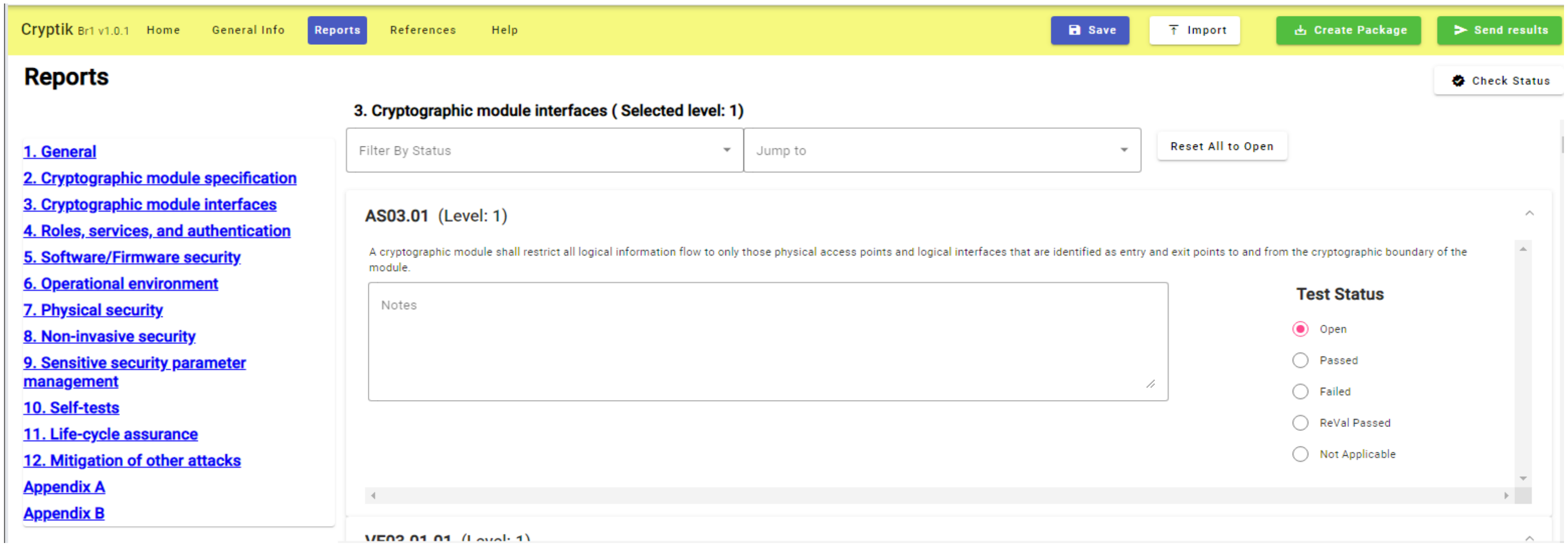
#	Package/File Names	Software/ Firmware Version	Non-Security Relevant Distinguishing Features	Integrity Test Implemented	Actions
	Package/File Names*	Software/ Firmware Version*	Non-Security Relevant Distinguishing Features	Integrity Test Implemented*	

Table 3. Tested Operational Environments – Software/Firmware/Hybrid

#	Operating System (Guest OS if Hypervisor)	Hardware Platform	Processor(s)	PAA/PAI	Hypervisor and Host OS	Version(s)	Actions
	Operating System*	Hardware Platform*	Processor(s)*	PAA/PAI*	Hypervisor and Host OS	Version(s)*	

Table 4. Vendor Affirmed Operational Environments – Software/Firmware/Hybrid

#	Operating System	Hardware Platform	Actions
	Operating System*	Hardware Platform*	



Reports

3. Cryptographic module interfaces (Selected level: 1)

- 1. General
- 2. Cryptographic module specification
- 3. Cryptographic module interfaces
- 4. Roles, services, and authentication
- 5. Software/Firmware security
- 6. Operational environment
- 7. Physical security
- 8. Non-invasive security
- 9. Sensitive security parameter management
- 10. Self-tests
- 11. Life-cycle assurance
- 12. Mitigation of other attacks
- Appendix A
- Appendix B

AS03.01 (Level: 1)

A cryptographic module shall restrict all logical information flow to only those physical access points and logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module.

Notes

Test Status

- ● Open
- ○ Passed
- ○ Failed
- ○ ReVal Passed
- ○ Not Applicable

VE03.01.01 (Level: 1)

Still to resolve…

- Long wait time from submission to validation.
- Modules are outdated by the time they are certified.
- Submitted reports are free form and not tied to test evidence.
- Manual review of submission by limited CMVP staffing.
- Repetitive information in multiple documents.

Automation of the CMVP (ACMVP)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURITY GUIDANCE

Automation of the NIST Cryptographic Module Validation Program

NIST established the Cryptographic Module Validation Program (CMVP) to ensure that hardware and software cryptographic implementations met standard security requirements. Since its start, the number and complexity of modules to be validated has increased steadily and now outstrips available human resources for product vendors, labs, and validators. This limits product options for many organizations required to use validated cryptography, especially federal agencies. NIST has started a broad effort to modernize and automate its cryptographic validation programs.

Program Goals:

- Automate the validation process.
- Design set of structured tests, schema and protocols for evidence submission.
- Streamline report review by eliminating manual check.

CMVP automation project

- ❖ Execution in phases; starting with software validation at security level 1.
- ❖ Project collaborators include product vendors and third-party labs.
- ❖ Bi-weekly meetings and regular tracking of project progress.
- ❖ Status so far:
  - ➢ TE classification based on documentation, code review and functional testing
  - ➢ Budling a standardized evidence catalog to be referenced in the report

ICMC conference 2023 clip

THANKS

рахмат
danke
謝謝
ngiyabonga
Баярлалаа
spas
teşekkür ederim
спасибо
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
faafetai lava
vinaka
dank je
misaotra
paldies
grazzi
спасибі
blagodaram
matondo
kiitos
dankie
thank you
gracias
хвала
nanni
nandri
dhanyavad
asante
manana
mauruuru
koszonom
obrigada
tenki
bedankt
hvala
gracie
bayarlalaa
aciū
dankon
akun
djiere dieuf
tau
mochchakkeram
murakoze
enkosi
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
gracies
sulpay
taiku
go raibh maith agat
chokrane
sobodi
dêkuji
obrigado
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
mèsi
didi madloba
ありがとう
tanemirt
grazie
najis tuke
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
merce
мерси
kam sah hamnida
rahmat
ευχαριστώ
merci
xiexie
তোমাকে ধন্যবাদ
감사합니다